IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MASSACHUSETTS

Joshua Willette, individually, and on behalf of all others similarly situated, Plaintiff, v. Anna Jaques Hospital d/b/a Beth Israel Lahey Health Anna Jaques Hospital, and Beth Israel Lahey Health, Inc., Defendants.	Case No. _____ **CLASS REPRESENTATION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Joshua Willette ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against the Defendants Anna Jaques Hospital d/b/a Beth Israel Lahey Health Anna Jaques Hospital ("AJH") and Beth Israel Lahey Health, Inc., ("Beth Israel" and collectively with AJH, "Defendants"). Plaintiff brings this action by and through his attorneys, and alleges, based upon personal knowledge as to his own actions, and based upon information and belief and reasonable investigation by his counsel as to all other matters, as follows.

I. INTRODUCTION

1. Defendants operate Anna Jaques Hospital, a hospital in Newburyport, MA.

2. As part of their operations, Defendants collects, maintains, and stores highly sensitive personal and medical information belonging to its patients, including, but not limited to their full names, Social Security numbers, dates of birth, addresses (collectively, "personally identifying information" or "PII"), health insurance information and other protected health information ("private health information" or "PHI"), as well as financial account/payment card information ("financial account information") (collectively, "Private Information").

3. On December 25, 2023, Defendants discovered that it had been the victim of a data breach incident in which unauthorized cybercriminals accessed its information systems and databases and stole Private Information belonging to Plaintiff and Class members (the "Data Breach").

4. On January 19, 2024, a ransomware gang claimed responsibility for the attack and demanded ransom for 600 GB of stolen patient data.

5. On January 26, 2024, after Defendants either declined or failed to pay the ransom, the full 600 GB of stolen data was published online, where it is still available for download.

6. Despite all these occurrences, Defendants did not begin sending notices to individuals whose information was accessed in the Data Breach until almost a full year after it discovered the Breach.

7. Because Defendants stored and handled Plaintiff's and Class members' highly-sensitive Private Information, they had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

8. Ultimately, Defendants failed to fulfill this obligation, as unauthorized cybercriminals breached Defendants' information systems and databases and stole vast quantities of Private Information belonging to AJH's patients, including Plaintiff and Class members. The Data Breach—and the successful exfiltration of Private Information—were the direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

9. The Data Breach occurred because Defendants failed to implement reasonable security protections to safeguard its information systems and databases. Thereafter, upon information and belief, Defendants failed to timely detect this Data Breach. Moreover, before the Data Breach occurred, Defendants failed to inform the public that its data security practices were

deficient and inadequate. Had Plaintiff and Class members been made aware of this fact, they would have never provided such information to AJH.

10. Defendants' subsequent handling of the breach was also deficient.

11. Defendants unreasonably delayed for nearly a year before disseminating notice and the meager attempt to ameliorate the effects of the Data Breach with two years of complimentary credit monitoring is woefully inadequate. Much of the Private Information that was stolen is immutable and two years of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

12. As a result of Defendants' negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;
- Charges and fees associated with fraudulent charges on their accounts; and
- The continued and increased risk of compromise to their Private Information, which remains in Defendants'possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Private Information.

13. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Defendants' failure to reasonably safeguard Plaintiff's and Class members' Private Information; its failure to reasonably provide timely notification to Plaintiff and Class members that their Private Information had been compromised; and for Defendants' failure to inform Plaintiff and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Joshua Willette

14. Plaintiff Joshua Willette is a resident and citizen of Newton Junction, New Hampshire. Plaintiff Willette was a patient at AJH. Plaintiff Willette received Defendants' Data Breach Notice.

Defendant Anna Jaques Hospital

15. Anna Jaques Hospital is a Massachusetts corporation with its principal place of business located at 25 Highland Ave, Newburyport, MA 01950. AJH conducts business in Massachusetts under the name Beth Israel Lahey Health Anna Jaques Hospital, as one of the hospitals in the Beth Israel health system.

Defendant Beth Israel Lahey Health, Inc.

16. Beth Israel Lahey Health, Inc. is a corporation with its principal place of business located at 20 University Road, Cambridge, MA 02138. Beth Israel jointly operates Beth Israel Health Anna Jaques Hospital with Defendant Anna Jaques Hospital.

III. JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at

least one Class member is a citizen of a state different from Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over Defendants because Defendants are each headquartered in Massachusetts.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District and because Defendants reside in this District.

IV. FACTUAL ALLEGATIONS

A. Anna Jaques Hospital – Background

20. Anna Jaques Hospital is a general hospital located in Newburyport, Massachusetts. As part of the normal operations, Defendants collects, maintains, and stores large volumes of Private Information belonging to current and former patients of AJH.

21. Defendants failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of AJH's current and former patients—Plaintiff and Class members.

22. Current and former patients of AJH, such as Plaintiff and Class members, made their Private Information available to Defendants with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

23. This expectation was objectively reasonable and based on an obligation imposed on Defendants by statute, regulations, industrial custom, and standards of general due care.

24. Unfortunately for Plaintiff and Class members, Defendants failed to carry out their duty to safeguard sensitive Private Information and provide adequate data security. As a result, they failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

25. According to Defendants' public statements and investigative reports, cybercriminals breached AJH's information systems some time before December 25, 2023. Defendants discovered this breach on December 25, 2023.

26. On January 19, 2024, the notorious ransomware gang Money Message claimed responsibility for the cyberattack, claiming that it stole more than 600GB of patient data from AJH, and demanded a ransom payment to be paid within one week. After Defendants failed to pay or declined to pay the ransom, the Money Message gang posted the entirety of the stolen data onto its leak site on January 26, 2024, where it is still available for download to this day.

27. On January 23, 2024, Defendants posted on AJH's website a vague notice concerning a possible data breach, but did not send direct notice to impacted individuals until almost a year later on December 5, 2024.

28. According to Defendants, the Breach exposed patients' names, addresses, medical information, health insurance information, Social Security number, driver's license number, financial information, and other personal or health information provided to AJH.

29. Defendants estimate that the Private Information belonging to at least 316,342 individuals was compromised in this incident.

C. Defendants' Many Failures Both Prior to and Following the Breach

30. Defendants collect and maintain vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations. The Data Breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

31. First, Defendants inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

32. Second, upon information and belief, Defendants failed to timely detect this data breach with Defendants' computer systems. Even nearly a year later, Defendants have still not disclosed when the breach actually occurred and Plaintiff and Class Members can only assume the worst. This presumed delayed detection provided these cybercriminals with potentially weeks or months to access and steal the sensitive Private Information belonging to Defendants' patients.

33. Third, Defendants failed to inform the public that their data security practices were deficient and inadequate. Had Plaintiff and Class members been aware that Defendants did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendants.

34. In addition to the failures that lead to the successful breach, Defendants' failings in handling the breach and responding to the incident exacerbated the resulting harm to the Plaintiff and Class members.

35. Defendants' nearly yearlong delay before informing victims of the Data Breach that their Private Information was compromised virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before the Plaintiff and Class members could take affirmative steps to protect their sensitive information.

As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

36. Additionally, Defendants' attempt to ameliorate the effects of this data breach with limited complimentary credit monitoring is woefully inadequate. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

37. In short, Defendants' myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiff and Class members that their personal and medical information had been stolen due to Defendants' security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiff's and Class members' Private Information for *at least* eleven-and-a-half months before Defendants finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

38. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

39. The Identity Theft Resource Center's ("ITRC") Annual End-of-Year Data Breach Report for 2023 listed 3,205 total compromises involving 353,027,892 victims.[1] This is nearly double the number of compromises in 2022, which had 1,802 total compromises involving 422,143,312 victims.[2] The 2022 figure was itself just 50 compromises short of the then record-breaking total of 1,852 set in 2021.[3] As it stands, the number of compromises in 2023 has managed to shatter 2021's record by a factor of 2.

40. The HIPAA Journal's 2023 Health Care Data Breach Report noted 725 data breaches involving 500 or more healthcare records.[4] In 2022, there were 707 compromises involving healthcare data in 2022 and 715 in 2021.[5]

41. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 3,205 in 2023.[6] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 353 million in 2023.[7]

---

[1] *2023 Data Breach Report*, Identity Theft Resource Center (January 2023), available at https://www.idtheftcenter.org/publication/2023-data-breach-report/.
[2] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.
[3] *Id.*
[4] Steve Adler, December 2023 Healthcare Data Breach Report, The HIPAA Journal (January 18, 2024), available at https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/.
[5] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.
[6] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2023*, Statista (Nov 9, 2024), available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed.
[7] *Id.*

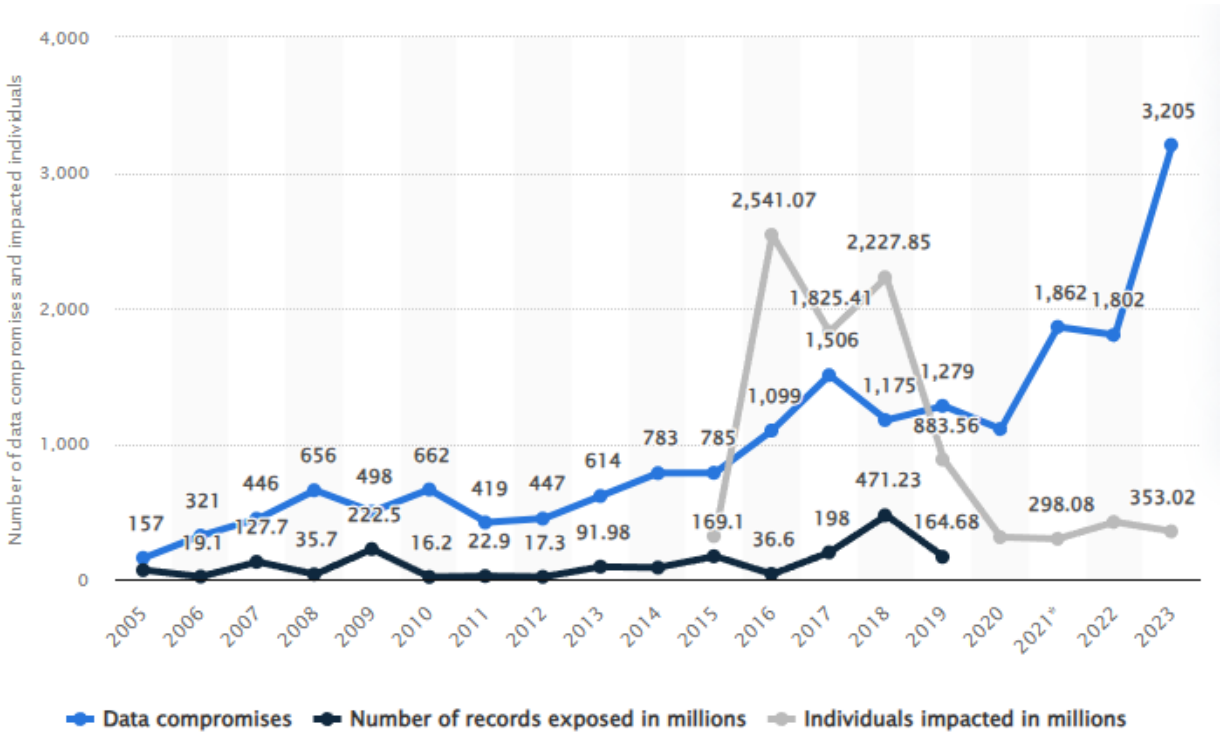

Figure 1 – *Chart of the Number of Data Breaches and Affected Individuals from 2005 to 2023.* [8]

42. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with online banking login information costing an average of $100, full credit card details and associated details costing between $10 and $100, and comprehensive data packages enabling complete identity theft selling for $1,000.[9]

43. In addition, the severity of the consequences of a compromised social security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory groups can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your

[8] *Id.*
[9] Ryan Smith, *Revealed-how much is personal information worth on the dark web?*, Insurance News (May 1, 2023), available at https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.

> good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[10]

This is exacerbated by the fact that the problems arising from a compromised social security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[11]

44. Further, as data breaches become ever more prevalent and as technology advances, computer programs can scan the internet to create a mosaic of information that could be used to link compromised information to an individual in ways in a phenomenon known as the "mosaic effect." By and through this process, names, dates of birth, and contact information such as telephone numbers and email addresses, hackers and identity thieves can access users' other accounts by, for example, bypassing security questions and 2FA security with the comprehensive collection of information at their disposal.

45. Thus, because of this effect, cybercriminals and other unauthorized parties could use Plaintiff's and Class Members' Private Information to access, inter alia, email accounts and

[10] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[11] *Id.*

financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members, even when that specific category of information is not compromised in a given breach.

46. A particularly trouble example of this effect is the development of "Fullz" packages. A "Fullz" package is a dosser of information that cybercriminals and other unauthorized parties can assemble by cross-referencing the Private Information compromised in a given data breach to publicly available data or data compromised in other data breaches. Automated programs can and are routinely used to create these dossiers and they typically represent an alarmingly accurate and complete profile of a given individual.

47. Therefore, through the use of these "Fullz" packages, stolen Private Information from this Data Breach can be easily linked to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. Thus, even if certain information such as emails, phone numbers, or credit card or financial account were not compromised in this Data Breach, criminals can easily create a Fullz package to sell for profit.

48. Upon information and belief, this has already transpired (and will continue to transpire) for Plaintiff and the Class. And any reasonable for any trier of fact will find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

49. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[12] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and social security numbers, which can be changed, medical records contain "a treasure trove of unalterable

[12] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[13] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[14] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[15] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[16]

50. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[17] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[18]

---

[13] *Id.*
[14] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/; *Data Breaches: In the Healthcare Sector*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited December 1, 2024).
[15] *Id.*
[16] *Id.*
[17] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[18] *Id.*

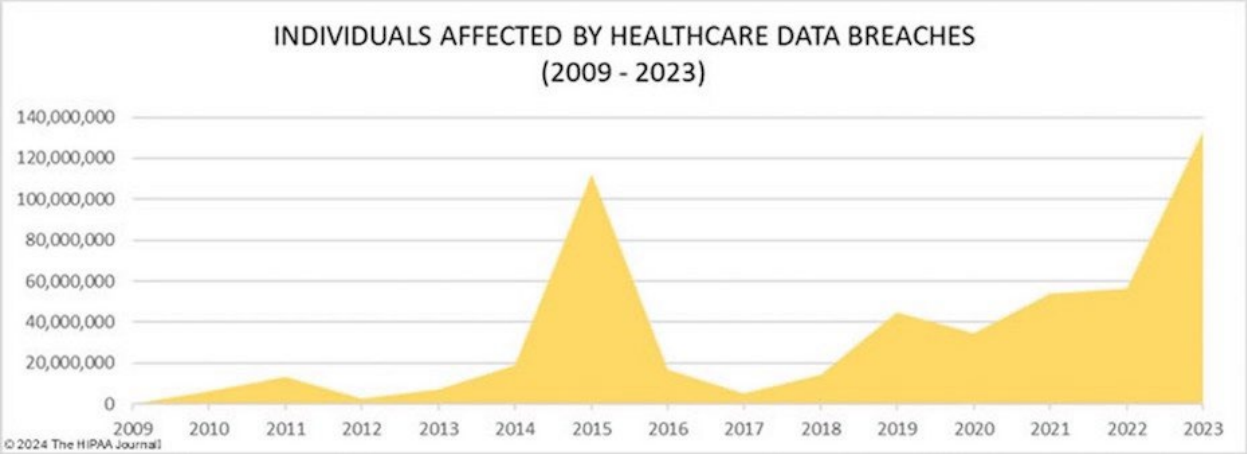

Figure 2 – *Chart of the Number of Individuals Affected by Healthcare Data Breaches from 2009 to 2023.*[19]

51. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendants charged with maintaining and securing patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendants knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[20]

52. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized

[19] *Healthcare fraud and the burden of medical ID theft*, Experian Health (February 14, 2024), available at https://www.experian.com/blogs/healthcare/healthcare-fraud-and-the-burden-of-medical-id-theft.
[20] *See, e.g.*, Steve Adler, *Healthcare Data Breach Statistics*, HIPAA Journal (November 25, 2024), available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.

these enforcement actions to place companies like Defendants on notice of their obligation to safeguard customer and patient information.[21]

53. Given the nature of the Data Breach, as well as the length of the time Defendants' networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' Private Information can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[22] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

55. To date, Defendants have offered its consumers only limited identity theft monitoring services. The services offered are inadequate to protect Plaintiff and Class members from the threats they will face for years to come, particularly in light of the Private Information at issue here.

56. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own

[21] *See, e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).
[22] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

acknowledgment of its duties to keep Private Information private and secure, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from misappropriation. As a result, the injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for its current and former patients.

E. Defendants Have a Duty and Obligation to Protect Private Information

57. Defendants have an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Plaintiff and Class members provided, and Defendants obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

58. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

59. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

60. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires entities to provide notice of a data breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

61. Defendants failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiff and Class members from unauthorized access and disclosure.

62. Upon information and belief, Defendants' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

63. Upon information and belief, Defendants also failed to store the information collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

64. Defendants also violated the HIPAA Breach Notification Rule since they did not inform Plaintiff and Class members about the breach until nearly a year after they discovered the breach.

2. FTC Act Requirements and Violations

65. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[23] The guidelines note businesses should protect the personal information

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed August 15, 2023).

that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[24] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25] Defendants clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

[24] *Id.*
[25] *Id.*

70. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

71. Defendants were fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiff and Class members. Defendants are sophisticated and technologically savvy businesses that relies extensively on technology systems and networks to maintain their practice, including storing patients' PII, protected health information, and medical information in order to operate their business.

72. Defendants had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendants and Plaintiff and Class members. Defendants alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

3. Industry Standards and Noncompliance

73. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

74. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting

which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

75. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

76. Defendants should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

77. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

4. Defendants' Own Stated Policies and Promises

78. Defendants' own published privacy policy states that it is "required by law to: make sure medical information that identifies you is kept private; give you this notice of our legal duties and privacy practices with respect to medical information about you; notify you if there is a breach of your unsecured personal health information; and follow the terms of the notice that is currently in effect." [26]

[26] *See* https://ajh.org/privacy-legal-notices/privacy-practices/ (last accessed Dec. 11, 2024).

79. Defendants failed to live up to their own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information belonging to Plaintiff and Class members.

F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

80. Like any data hack, the Data Breach presents major problems for all affected.[27]

81. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[28]

82. The ramifications of Defendants' failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

83. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

84. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

85. Accordingly, Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing

[27] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.
[28] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.[29] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[30]

86. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

87. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[31] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[32]

88. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[33] Medical Identity Theft is especially

[29] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[30] *Id.*
[31] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.
[32] *Id.*
[33] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[34]

89. In response to the Data Breach, Defendants offered to provide certain individuals whose Private Information was exposed in the Data Breach with 24 months of credit monitoring. However, this is inadequate to protect victims of the Data Breach from the lifelong risk of harm imposed on them by Defendants' failures.

90. Moreover, the credit monitoring offered by Defendants is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

91. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken

[34] *Id.*

from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendants' delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

92. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within the limited time of credit monitoring offered by Defendants.

93. As a direct and proximate result of Defendants' acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

94. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFF

Joshua Willette

95. Plaintiff Joshua Willette is a patient of AJH.

96. Plaintiff Willette received Defendants' Data Breach notice. The notice informed Plaintiff Willette that his Private Information was improperly accessed and obtained by third parties in the Data Breach.

97. Following the Data Breach, Plaintiff experienced a dramatic increase in the number of spam calls.

98. As a result of the Data Breach, Plaintiff Willette has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Willette has also spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

99. As a result of the Data Breach, Plaintiff Willette has suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his Private Information for purposes of identity theft and fraud. Plaintiff Willette is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

100. Plaintiff Willette suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from her; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

101. As a result of the Data Breach, Willette anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

102. Plaintiff brings this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendants their executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

103. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendants and obtainable by Plaintiff only through the discovery process. On information and belief, the number of affected individuals estimated to be 316,342. The members of the Class will be identifiable through information and records in Defendants' possession, custody, and control.

104. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendants learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendants' response to the Data Breach was adequate;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

f. Whether Defendants owed a duty to safeguard their Private Information;

g. Whether Defendants breached the duty to safeguard Private Information;

h. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

i. Whether Defendants breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

j. Whether Defendants' conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants' conduct was *per se* negligent;

m. Whether Defendants were unjustly enriched;

n. What damages Plaintiff and Class members suffered as a result of Defendants' misconduct;

o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief.

105. Typicality: Plaintiff's claims are typical of the claims of the Class as Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendants' uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Defendants acted, and refused to act, on grounds generally applicable to the Class.

106. Adequacy: Plaintiff is an adequate class representative because his interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, he has retained counsel competent and highly experienced in complex class action litigation, and Plaintiff

intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

107. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants' records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiff on behalf of the Class)

108. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

109. Defendants owe a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendants also owe several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

110. Defendants owe this duty because it had a special relationship with Plaintiff's and Class members. Plaintiff and Class members entrusted their Private Information to Defendants on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendants had the ability to protect their systems and the Private Information stored on them from attack.

111. Defendants also owe this duty because industry standards mandate that Defendants protect patients' confidential Private Information.

112. Defendants also owe a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and Class members. This duty exists to provide Plaintiff and Class members with the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

113. Defendants breached the duties owed to Plaintiff and Class members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their Private Information.

114. Defendants also breached the duties owed to Plaintiff and Class members by failing to timely and accurately disclose to them that their Private Information had been improperly acquired and/or accessed.

115. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanent increased risk of identity theft.

116. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Defendants and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

117. In failing to provide prompt and adequate individual notice of the Data Breach, Defendants also acted with reckless disregard for the rights of Plaintiff and Class members.

118. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen the data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiff on behalf of the Class)

119. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

120. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a duty on Defendants to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiff and Class members.

121. HIPAA imposes a duty on Defendants to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information. 42 U.S.C. § 1302(d), *et seq*.

122. HIPAA also requires Defendants to render unusable, unreadable, or indecipherable all Private Information it collected. Defendants were required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

123. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

124. Defendants violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' Private Information.

125. Defendants violated HIPAA by failing to properly encrypt the Private Information collected.

126. Defendants violated HIPAA by unduly delaying reasonable notice of the actual breach; in this case by almost a year.

127. Defendants' failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

128. Plaintiff and Class members are within the class of persons that the FTCA and HIPAA are intended to protect.

129. It was reasonably foreseeable that the failure to protect and secure Plaintiff's and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

130. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

131. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen the data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Class)

132. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

133. Plaintiff and Class members provided Defendants with their Private Information.

134. By providing their Private Information, and upon Defendants' acceptance of this information, Plaintiff and the Class, on one hand, and Defendants, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

135. The implied contracts between Defendants and Plaintiff and Class members obligated Defendants to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above.

136. The implied contracts for data security also obligated Defendants to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

137. Defendants breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

138. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Class)

139. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

140. This count is brought in the alternative to Count III.

141. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendants.

142. Plaintiff and the Class conferred their Private Information to Defendants as part of receiving medical care. Plaintiff and the Class also conferred payment to Defendants in exchange for medical services.

143. Plaintiff and Class members conferred their Private Information alongside payment with the understanding that the payment was, in part, to be used to implement data security sufficient to adequately protect their Private Information. And this payment represented a benefit that was to be used for a specific purpose.

144. Defendants, as a health care service providers, received payment from patients to handle and manage this Private Information. Plaintiff and Class members conferral of their Private Information was a direct benefit since Defendants were able to use this information for business purposes and financial gain. There was an understanding that a portion of the monies Defendants received from the use of this Private Information, was intended to be used to implement data security sufficient to adequately protect this Private Information.

145. Defendants understood that they was so benefitted.

146. However, instead of providing a reasonable level of security, training, protocols, and other measures that would have prevented the Data Breach, as described in detail above, Defendants, upon information and belief, knowingly and opportunistically elected to increase their own profits at the expense of Plaintiff and Class members by not expending the money required to do so.

147. And in failing to expend the monies conferred with the express understanding that it would be used on data security, Defendants knowingly and deliberately enriched themselves at the expense of Plaintiff and Class members.

148. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner.

149. Defendants are therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendants as a result of its wrongful conduct, including specifically the value to Defendants of the Private Information that was accessed and exfiltrated in the Data Breach and the profits Defendants received from the use and sale of that information. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from its wrongful conduct.

COUNT V
BREACH OF FIDUCIARY DUTY
(By Plaintiff on behalf of the Class)

150. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

151. Plaintiff brings this claim on behalf of themselves and the Class.

152. Plaintiff and Class members provided their Private Information to Defendants in confidence with the reasonable belief that Defendants would protect their information. Plaintiff and Class members would not have provided their information to Defendants had they known Defendants would fail to adequately protect their information.

153. In collecting and maintaining this Private Information, Defendants created a fiduciary relationship between themselves and Plaintiff and Class members. As such, Defendants owed a duty to *primarily* act for the benefit of its current and former patients upon matters within the scope of their relationship. This included a duty to protect Plaintiff's and Class Members' Private Information.

154. These fiduciary duties and responsibilities are also described under the procedures set forth in the HIPAA Privacy Rule, including the procedures and definitions found in 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which requires Defendants to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient information and to secure the health care information they maintain and to keep it free from disclosure.

155. Defendants breached these fiduciary duties by failing to implement adequate safeguards and causing Plaintiff's and Class members' Private Information to be disclosed to unauthorized third parties.

156. As a direct and proximate result of Defendants' breaches of its fiduciary duties and the resulting disclosure of Plaintiff and Class member's Private Information, Plaintiff and Class members have suffered damages, including, but not limited to exposure to heightened future risk of identity theft, loss of privacy, confidentiality, emotional distress and humiliation.

COUNT VI
INVASION OF PRIVACY
(By Plaintiff on behalf of the Class)

157. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

158. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that Defendants possessed and/or continues to possess.

159. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendants invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

160. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Defendants' actions highly offensive.

161. Defendants invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

162. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

163. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendants have acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing their own economic, corporate, and legal interests above the privacy interests of millions of patients. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of himself and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative Class, demands a trial by jury on all issues so triable.

Date: January 7, 2025

Respectfully Submitted,

By: */s/ James J. Reardon*

James J. Reardon (BBO# 566161)
REARDON SCANLON LLP
45 South Main Street, 3rd Floor
West Hartford, CT 06107
T: (860) 944-9455
james.reardon@reardonscanlon.com

Daniel O. Herrera*
Nickolas J. Hagman*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

* *Pro Hac Vice* forthcoming

Attorneys for Plaintiff and the Proposed Class